CFO 15431 US / SUG

09/867,470
GAU: 2151

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００１年　５月１１日

出願番号
Application Number:　特願２００１－１４１７７４

出願人
Applicant(s):　キヤノン株式会社

２００１年　６月２６日

特許庁長官
Commissioner,
Japan Patent Office　及川耕造

出証番号　出証特２００１－３０６０２２４

【書類名】　特許願

【整理番号】　4462021

【提出日】　平成13年 5月11日

【あて先】　特許庁長官殿

【国際特許分類】　H04N 1/00

【発明の名称】　ネットワークシステム、Ｗｅｂサーバへのアクセス制限方法、記憶媒体、ネットワークデバイス及びその制御方法、並びにプログラム

【請求項の数】　14

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

【氏名】　横倉　秀則

【特許出願人】

【識別番号】　000001007

【氏名又は名称】　キヤノン株式会社

【代表者】　御手洗　冨士夫

【代理人】

【識別番号】　100081880

【弁理士】

【氏名又は名称】　渡部　敏彦

【電話番号】　03(3580)8464

【先の出願に基づく優先権主張】

【出願番号】　特願2000-176128

【出願日】　平成12年 6月12日

【手数料の表示】

【予納台帳番号】　007065

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9703713

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワークシステム、Ｗｅｂサーバへのアクセス制限方法、記憶媒体、ネットワークデバイス及びその制御方法、並びにプログラム

【特許請求の範囲】

【請求項１】　複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの１つがＷｅｂクライアントを搭載しており、前記コンピュータの他の１つ及び前記ネットワークデバイスの１つの一方がＷｅｂサーバを搭載しているネットワークシステムにおいて、前記Ｗｅｂサーバは、前記Ｗｅｂサーバへのアクセスを制限することを決定する決定手段と、前記Ｗｅｂサーバへのアクセスを制限することが決定されたときに、前記Ｗｅｂサーバへのアクセスが制限されていることを示すデータを前記Ｗｅｂクライアントに通知する通知手段とを備えることを特徴とするネットワークシステム。

【請求項２】　前記通知手段は、前記Ｗｅｂサーバへのアクセスを制限することが決定されたとき、且つ前記Ｗｅｂクライアントが前記データの更新日付を指定したときに、当該更新日付以降に前記データが更新されているか否かに拘わらず、前記Ｗｅｂサーバへのアクセスが制限されていることを示すデータを前記Ｗｅｂクライアントに通知することを特徴とする請求項１記載のネットワークシステム。

【請求項３】　前記Ｗｅｂサーバは、前記ネットワークデバイスの１つに搭載されていることを特徴とする請求項２記載のネットワークシステム。

【請求項４】　前記Ｗｅｂサーバは、前記コンピュータの他の１つに搭載され、且つ、前記複数のネットワークデバイスの状況を前記Ｗｅｂクライアントに通知する他の通知手段を備えることを特徴とする請求項２記載のネットワークシステム。

【請求項５】　複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの１つがＷｅｂクライアントを搭載しており、前記コンピュータの他の１つ及び前記ネットワークデバイスの１つの一方がＷｅｂサーバを搭載しているネットワークシステムにおける

Ｗｅｂサーバへのアクセス制限方法において、前記Ｗｅｂサーバへのアクセスを制限することを決定する決定工程と、前記Ｗｅｂサーバへのアクセスを制限することが決定されたときに、前記Ｗｅｂサーバへのアクセスが制限されていることを示すデータを前記Ｗｅｂクライアントに通知する通知工程とを備えることを特徴とするＷｅｂサーバへのアクセス制限方法。

【請求項６】　前記通知工程は、前記Ｗｅｂサーバへのアクセスを制限することが決定されてたとき、且つ前記Ｗｅｂクライアントが前記データの更新日付を指定したときに、当該更新日付以降に前記データが更新されているか否かに拘わらず、前記Ｗｅｂサーバへのアクセスが制限されていることを示すデータを前記Ｗｅｂクライアントに通知することを特徴とする請求項５記載のＷｅｂサーバへのアクセス制限方法。

【請求項７】　前記Ｗｅｂサーバは、前記ネットワークデバイスの１つに搭載されていることを特徴とする請求項６記載のＷｅｂサーバへのアクセス制限方法。

【請求項８】　前記Ｗｅｂサーバは、前記コンピュータの他の１つに搭載され、且つ、前記複数のネットワークデバイスの状況を前記Ｗｅｂクライアントに通知する他の通知工程を備えることを特徴とする請求項６記載のＷｅｂサーバへのアクセス制限方法。

【請求項９】　複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの１つがＷｅｂクライアントを搭載しており、前記コンピュータの他の１つ及び前記ネットワークデバイスの１つの一方がＷｅｂサーバを搭載しているネットワークシステムにおけるＷｅｂサーバへのアクセス制限方法を実行するプログラムを記憶した読み出し可能な記憶媒体であって、前記Ｗｅｂサーバへのアクセス制限方法は、前記Ｗｅｂサーバへのアクセスを制限することを決定する決定工程と、前記Ｗｅｂサーバへのアクセスを制限することが決定されたときは、前記Ｗｅｂサーバへのアクセスが制限されていることを示すデータを前記Ｗｅｂクライアントに通知する通知工程とを備えることを特徴とする記憶媒体。

【請求項１０】　ネットワークに接続されたネットワークデバイスにおいて

、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別手段と、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信手段とを備えることを特徴とするネットワークデバイス。

【請求項１１】　更に、前記他のネットワークデバイスからの日時情報を検出する検出手段を備え、前記送信手段は、前記他のネットワークデバイスからのアクセスを制限しないときは、前記検出された日時情報に応じて前記ネットワークデバイスのステータスを示す情報を前記他のネットワークデバイスに送信することを特徴とする請求項１０記載のネットワークデバイス。

【請求項１２】　更に、前記他のネットワークデバイスからの日時情報を検出する検出手段を備え、前記送信手段は、前記他のネットワークデバイスからのアクセスを制限するときは、前記検出された日時情報に拘わらず前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信することを特徴とする請求項１０記載のネットワークデバイス。

【請求項１３】　ネットワークに接続されたネットワークデバイスの制御方法において、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別工程と、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信工程とを備えることを特徴とするネットワークデバイスの制御方法。

【請求項１４】　ネットワークに接続されたネットワークデバイスの制御方法を実行するプログラムにおいて、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別ステップと、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信ステップとを含むことを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークシステム、Ｗｅｂサーバへのアクセス制限方法、記憶媒体、ネットワークデバイス及びその制御方法、並びにプログラムに関する。

【０００２】

【従来の技術】

近年、複数のコンピュータや複数のプリンタ等のネットワークデバイスが接続されたネットワークを介して行われるインターネットが急速に普及し、このインターネットを利用した様々なアプリケーションが開発されている。将来的には、このインターネット利用技術は急速に進むことが予想されている。その中で、ネットワークに接続されるプリンタ等のネットワークデバイスにＷｅｂサーバの機能を搭載することにより、ネットワークデバイスにアクセスして、ネットワークデバイスのステータスや印刷ジョブ等を市販のＷｅｂブラウザを用いて参照することができる製品が開発されている。このようなネットワークデバイスでは、その初期設定値等がデバイス管理者により設定されている。デバイス管理者は、ネットワークデバイスのメンテナンス中などに設定がユーザによって書き換えられるのを防止するためにＷｅｂサーバへのアクセスを制限する手立てを講じる必要がある。

【０００３】

【発明が解決しようとする課題】

しかしながら、Ｗｅｂサーバへのアクセスを制限し、アクセスが禁止されているユーザからのアクセスを受けた場合に、403 Forbidden等のエラーコードを該ユーザに送信することでアクセスが制限されていることを通知することも可能であるが、このエラーコードでは情報量が乏しいため、Ｗｅｂサーバへのアクセスを制限した理由がユーザに明確に通知することができない。

【０００４】

また、ＨＴＭＬファイルを動的に変更することによりＷｅｂサーバへのアクセスが制限されている旨を通知することも可能であるが、Ｗｅｂサーバへアクセスしたときは、ＨＴＭＬファイルの更新日付指定の如何に拘わらず、ユーザ側のＷｅｂブラウザでキャッシュしていたＨＴＭＬファイルを表示してしまい、更新日

付以降にＨＴＭＬファイルが更新されていた場合であっても、表示データの量を低減することができない。

【０００５】

本発明の目的は、ネットワークデバイスへの最新のアクセス制限の理由を明確、且つ確実にユーザに通知することができ、また、ユーザに通知する表示用データの量を低減することにある。

【０００６】

【課題を解決するための手段】

上記目的を達成するために、ネットワークシステムは、複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの１つがＷｅｂクライアントを搭載しており、前記コンピュータの他の１つ及び前記ネットワークデバイスの１つの一方がＷｅｂサーバを搭載しているネットワークシステムにおいて、前記Ｗｅｂサーバは、前記Ｗｅｂサーバへのアクセスを制限することを決定する決定手段と、前記Ｗｅｂサーバへのアクセスを制限することが決定されたときに、前記Ｗｅｂサーバへのアクセスが制限されていることを示すデータを前記Ｗｅｂクライアントに通知する通知手段とを備えることを特徴とする。また、そこで使われるＷｅｂサーバへのアクセス制限方法、該アクセス制限方法を実行するプログラムを記憶した記憶媒体を提供する。

【０００７】

上記目的を達成するために、ネットワークデバイスは、ネットワークに接続されたネットワークデバイスにおいて、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別手段と、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信手段とを備えることを特徴とする。また、その制御方法、該制御方法を実行するプログラムを提供する。

【０００８】

【発明の実施の形態】

以下、本発明の実施の形態に係るネットワークシステムを図面を参照して説明する。

【０００９】

図１は、本発明の実施の形態に係るネットワークシステムの構成図である。

【００１０】

図１において、ＬＡＮ１００（ネットワーク）には、カラープリンタ１０１、ネットワークプリンタとして使用可能なコピー機等のＭＦＰ（Multi Function Peripheral）１０２、モノクロプリンタ１０３、ファクシミリ１０４、及びスキャナ１０５，１０６から成る複数のネットワークデバイスと、デスクトップＰＣ１１１，１１２及びノートＰＣ１１３から成る複数のコンピュータとが接続されている。カラープリンタ１０１、ＭＦＰ１０２、モノクロプリンタ１０３、ファクシミリ１０４、及びデスクトップＰＣ１１１，１１２は、ビルの２階に配されており、スキャナ１０５，１０６及びノートＰＣ１１３は、ビルの１階に配されている。ノートＰＣ１１３は、ポータブルであるので、ＬＡＮ１００から外されることもあり得る。

【００１１】

デスクトップＰＣ１１１，１１２及びノートＰＣ１１３には、夫々、Ｗｅｂサーバ機能を搭載したネットワークデバイスのステータス（状況）等を参照するＷｅｂブラウザが搭載されており、これらのＰＣは、ネットワークデバイス間でＨＴＭＬ（Hypertext Markup Language）文書を送受信するためのＨＴＴＰ（Hyper text Transfer Protocol）によるアクセスが可能である。

【００１２】

上記ネットワークデバイスの少なくとも１つには、Ｗｅｂサーバ（Ｗｅｂサーバ機能）が搭載されており、コンピュータの少なくとも１つには、Ｗｅｂクライアント（Ｗｅｂクライアント機能）が搭載されている。

【００１３】

更に、ネットワーク１００は、ファイアウォール１２０を介してインターネット１３０に接続されており、インターネット１３０を介して他のネットワーク１４０とも接続されている。

【００１４】

図２は、図１のネットワークシステムにおけるネットワークデバイスの内部構成のブロック図である。

【００１５】

図２において、Ｗｅｂサーバ機能を搭載するネットワークデバイスは、制御部２００、周辺機器制御部２０１、及びＬＡＮプロトコル制御部２０２を有しており、これらは、各制御部を総括的に制御する制御バス２０３に夫々接続されていると共に、データバス２０４にも夫々接続されている。データバス２０４には、プリンタやファクシミリ等の周辺機器が接続されている。また、制御部２００は、ＣＰＵ、ＲＯＭ、ＲＡＭ、バックアップＲＡＭ等で構成されている。例えば、ＣＰＵは、ＲＯＭに格納されているプログラムに従ってネットワークデバイスがメンテナンス中か否かを判別し、メンテナンス中である場合はアクセス制限を行うと判断する。なお、バックアップＲＡＭには、ＣＰＵがアクセス制限するか否かを判断するためのフラグが格納されている。周辺機器制御部２０１は、データバス２０４を介してプリンタやファクシミリ等の周辺機器にデータを送受信する。ＬＡＮプロトコル制御部２０２には、ＬＡＮ１００を介して他のネットワーク機器又は他のＰＣと双方向にデータを送受信する。

【００１６】

図３は、本発明の実施の形態に係るネットワークシステムが実行するＷｅｂサーバ機能を搭載したネットワークデバイスへのアクセス制限処理のフローチャートである。

【００１７】

図３において、Ｗｅｂサーバ機能を搭載するネットワークデバイス（以下「Ｗｅｂサーバ」という。）の起動後に、Ｗｅｂクライアント機能を搭載するコンピュータ（以下「Ｗｅｂクライアント」という。）からＷｅｂサーバへのアクセスがなされると（ステップＳ３００でＹＥＳ）、ＷｅｂサーバはＷｅｂサーバ本体の格納手段に格納されているアクセス制限情報の参照を行い（ステップＳ３０１）、Ｗｅｂクライアントからのアクセスを制限するか否か判別する（ステップＳ３０２）（判別・決定手段）。上記アクセス制限情報は、ネットワークデバイス

のデバイス管理者が設定した、当該ネットワークデバイスのＷｅｂサーバへのアクセス制限を判断するための情報である。

【００１８】

ステップＳ３０２の判別の結果、アクセス制限情報によりＷｅｂクライアントからのアクセスを制限しないときは（アクセスを許可するとき）、ステップＳ３０３に進んで、Ｗｅｂクライアントから「If-Modified-Since」要求があるか否かを判別する。ここで、「If-Modified-Since」要求とは、Ｗｅｂクライアントから送出される日付（日時）情報付きの要求であって、その日付（日時）以降にＷｅｂサーバのＨＴＭＬファイルが更新されていなければ、ＨＴＭＬファイル更新されていないことを示す「Not Modified」を送信することにより、ネットワークの受信負荷を削減するためのものである。また、Ｗｅｂクライアントは、ユーザの指定したＵＲＬに相当するファイルを既にキャッシュしている場合に、この「If-Modified-Since」要求を送出する。

【００１９】

ステップＳ３０３の判別の結果、Ｗｅｂクライアントから「If-Modified-Since」要求があるときは、ステップＳ３０４に進んで、「If-Modified-Since」に付加されてきた日付（日時）情報を検出し（検出手段）、該日時情報を用いてＷｅｂクライアントが保持しているＨＴＭＬファイルの日時情報と比較して、Ｗｅｂサーバが保持しているＨＴＭＬファイルが更新されているか否かを判別する（ステップＳ３０４）。ステップＳ３０４の判別の結果、Ｗｅｂクライアントが通知してきた日付（日時）以降にファイルが更新されていないときは、ＨＴＭＬファイルの変更がされていないことを示す「Not Modified」をＷｅｂクライアントに送信する（ステップＳ３０５）。一方、ＨＴＭＬファイルが更新されているときは、後述する図５（ａ）に対応するＨＴＭＬファイルのデータ（デバイス情報）を更新したファイルとしてＷｅｂクライアントに送信して（ステップＳ３０６）、本処理を終了する。ステップＳ３０６では、特に指定されていなければ、ネットワークデバイスで特定されているＴｏｐページのＨＴＭＬファイルを送信する。

【００２０】

ステップＳ３０３の判別の結果、Ｗｅｂクライアントから「If-Modified-Since」要求がないときは、ＨＴＭＬファイルが更新されているか否かに拘わらず、後述する図５（ａ）に対応するＨＴＭＬファイルのデータ（デバイス情報）をＷｅｂクライアントに送信して（ステップＳ３０６）、本処理を終了する。

【００２１】

ステップＳ３０２の判別の結果、アクセス制限情報によりＷｅｂクライアントからのアクセスを制限するときは（アクセスを許可しないとき）、ステップＳ３０７に進んで、Ｗｅｂクラアントから「If-Modified-Since」要求があるか否かを判別し、「If-Modified-Since」要求がないときは、予め用意しておいたＷｅｂサーバへのアクセス制限及びその理由を示す情報、すわなち後述する図５（ｂ）に対応するＨＴＭＬファイル（図５（ｂ））のデータ（デバイス情報）をＷｅｂクライアントに送信することにより、アクセスが制限されていることをユーザに通知して（ステップＳ３０８）（通知・送信手段）、本処理を終了する。一方、ステップＳ３０７の判別の結果、「If-Modified-Since」要求があるときは、Ｗｅｂクライアントが保持しているＨＴＭＬファイルの日時以降にＷｅｂサーバが保持しているＨＴＭＬファイルが更新されているか否かの判別を行うことなく（ステップＳ３０９）、上記ステップＳ３０８の処理を実行して、本処理を終了する。

【００２２】

図４は、Ｗｅｂクライアント及びＷｅｂサーバ間のＨＴＴＰシーケンスの一例を示す図である。以下の説明では、図３のフローチャートにおけるステップ番号の付記により、図３の説明と対応させている。

【００２３】

図４において、カラープリンタ１０１、ＭＦＰ１０２、モノクロプリンタ１０３、及びファクシミリ１０４等のネットワークデバイスの少なくとも１つには、Ｗｅｂサーバ４０１が搭載されている。また、デスクトップＰＣ１１１，１１２及びノートＰＣ１１３の少なくとも１つには、Ｗｅｂクライアント４００が搭載されている。

【００２４】

まず、Ｗｅｂクライアント４００に、デスクトップＰＣ１１１，１１２及びノートＰＣ１１３等に搭載されているＷｅｂブラウザからパケットが送信され、そのＷｅｂブラウザのＵＲＬで特定のＷｅｂサーバ４０１を指定したときに、そのＷｅｂサーバ４０１のＴｏｐページの情報をＷｅｂクライアント４００が保持していたならば、Ｗｅｂクラアント４００は、データ取得要求としてGET / HTTP/1.0 If-Modified-Since: Tuesday, 30-Feb-00... により、Ｗｅｂサーバ４０１へのアクセスの制限がなされているか否かの問い合わせを開始する（４０２）（図３のステップＳ３００）。

【００２５】

次いで、Ｗｅｂサーバ４０１は、GET Ackを返信することにより、Ｗｅｂクライアント４００に対して、データを確実に取得したことを通知する（４０３）と共に、データ取得要求（４０２）に対するＷｅｂサーバ４０１のステータスを検出された日時情報に応じて返信する（４０４）（図３のステップＳ３０２，Ｓ３０７）。ここでは、正常なステータスを示す情報であるHTTP/1.0 200 OKを返信し、その後、<html>.<head>... __err.gif...により、Ｗｅｂサーバ４０１へのアクセスが制限されていることを示すＨＴＭＬファイルを返信する（４０５）（図３のステップＳ３０８）。ここでは、ＨＴＭＬファイルが画像データファイル__err.gifを含んでいるので、Ｗｅｂクラアント４００は、GET /__err.gif HTTP/1.0 ... により、画像データファイル__err.gifの取得を要求し（４０６）、Ｗｅｂサーバ４０１は、その要求に対する応答として後述する図５（ｂ）に対応するＨＴＭＬファイルをＷｅｂクライアント４００に対して送信する（４０７）。

【００２６】

図５は、Ｗｅｂサーバへアクセスした場合のＷｅｂブラウザの表示例を示す図であり、（ａ）は一般的なＷｅｂブラウザの場合、（ｂ）はＷｅｂサーバへのアクセスが制限されている場合である。

【００２７】

まず、図５（ａ）において、Ｗｅｂブラウザ５００は、一般的なＷｅｂブラウザの画面５０２を示しており、ＩＰアドレスを指定してネットワークデバイスを特定するＵＲＬ５０１を含む。本例では、プリンタの画像と、このステータスが

表示されている。なお、ファイル名を特に指定しない場合には、Ｗｅｂサーバ４０１が保持しているＴｏｐページのデータを表示する。

【００２８】

一方、図５（ｂ）において、Ｗｅｂブラウザ５０３は、デバイス管理者が、Ｗｅｂサーバ４０１へのアクセスを制限している場合にＷｅｂサーバ４０１から送信される画面５０５を示している。画面５０５上の画像データや文字データにより、Ｗｅｂサーバ４０１へのアクセスが制限された状態であることをＷｅｂクライアント４００に明確に通知することができる。

【００２９】

Ｗｅｂブラウザ５００，５０３としては、代表的なものとしては、マイクロソフト社のInternet Explorerや、ネットスケープ社のNetscape Communicator等が挙げられる。

【００３０】

本実施の形態によれば、Ｗｅｂサーバへのアクセスを制限することが決定しているときに（ステップＳ３０２でＹＥＳ）、Ｗｅｂサーバへのアクセスが制限されていること、及びその理由を示すＨＴＭＬファイル（図５（ｂ））のデータをＷｅｂクライアントに通知する（ステップＳ３０８）ので、Ｗｅｂクライアントに通知されたＨＴＭＬファイルによって、Ｗｅｂサーバへのアクセス制限及びその理由（メンテナンス中など）をユーザに確実に通知することができる。また、Ｗｅｂサーバへのアクセスを制限することが決定しているとき（ステップＳ３０２でＹＥＳ）、且つＷｅｂクライアントがデータの更新日付を指定しているときに（ステップＳ３０７でＹＥＳ）、ＨＴＭＬファイルの更新日時比較を行うことなく（ステップＳ３０９）、Ｗｅｂサーバへのアクセスが制限されていること、及び、その理由を示すＨＴＭＬファイル（図５（ｂ））をＷｅｂクライアントに通知する（ステップＳ３０８）ので、ＷｅｂブラウザでキャッシュしていたＨＴＭＬファイルを表示するのを防止でき、確実に最新の理由等を通知することができる。また、アクセス制限がされていない場合は、検出された日時情報（更新日時）に応じてＷｅｂサーバのステータスを示す情報をＷｅｂクライアントに送信するので、表示データの量を低減することができる。

【００３１】

なお、上記実施の形態において、デバイス情報の通知をＨＴＭＬファイルにより行っているが、テキストファイルや画像ファイル等によって行ってもよい。また、上記実施の形態において、Ｗｅｂサーバ機能がネットワークデバイスに搭載されているが、Ｗｅｂサーバ機能がコンピュータに搭載されて、プロキシサーバの役割を担うことにより、デバイス情報をＷｅｂクライアントに送信してもよい。また、Ｗｅｂクライアント機能を搭載したネットワークデバイスと、Ｗｅｂサーバ機能を搭載したネットワークデバイスとの間で上記図３の処理及び図４のシーケンスを行ってもよい。

【００３２】

上記実施の形態では、Ｗｅｂサーバへのアクセス制限処理を説明したが、この処理をプログラムとして書き込み、装置で該記憶媒体から上記プログラムを読み出して実行しても、上述した処理を実行することができる。また、記憶媒体は、フロッピー（登録商標）ディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ等の様々なものが考えられるが、特定のものに限定する必要はなく、上記プログラムを記憶できるものであればよい。

【００３３】

【発明の効果】

以上詳細に説明したように、本発明によれば、Ｗｅｂサーバ等のネットワークデバイスへの最新のアクセス制限の理由を明確、且つ確実にユーザに通知することができ、また、ユーザに通知する表示用データの量を低減することができる。

【００３４】

例えば、アクセスを制限する場合は、Ｗｅｂブラウザでキャッシュしていた ＨＴＭＬファイルを表示するのを確実に防止することができる。さらに、Ｗｅｂブラウザでキャッシュしている ＨＴＭＬファイルの日時情報に応じて、該ＨＴＭＬファイルを表示させるので、ユーザに通知する表示用データの量を低減することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係るネットワークシステムの構成図である。

【図２】

図１のネットワークシステムにおけるネットワークデバイスの内部構成のブロック図である。

【図３】

本発明の実施の形態に係るネットワークシステムが実行するＷｅｂサーバ機能を搭載したネットワークデバイスへのアクセス制限処理のフローチャートである。

【図４】

Ｗｅｂクライアント及びＷｅｂサーバ間のＨＴＴＰシーケンスの一例を示す図である。

【図５】

Ｗｅｂサーバへアクセスした場合のＷｅｂブラウザの表示例を示す図であり、（ａ）は一般的なＷｅｂブラウザの場合、（ｂ）はＷｅｂサーバへのアクセスが制限されている場合である。

【符号の説明】

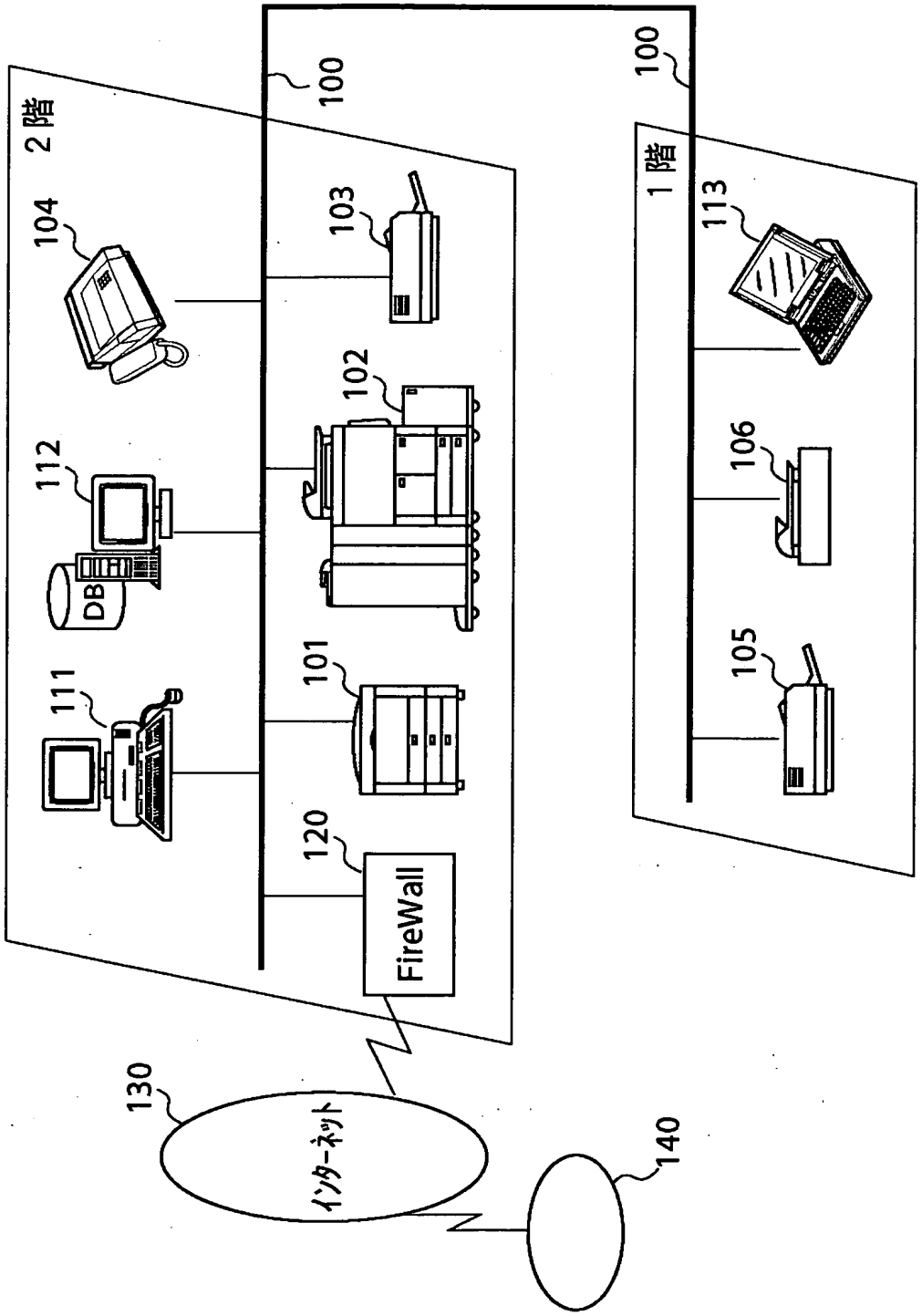
１００，２０５　ＬＡＮ
１０１　カラープリンタ
１０２　ＭＦＰ
１０３　モノクロプリンタ
１０４　ファクシミリ
１０５，１０６　スキャナ
１１１，１１２　デスクトップＰＣ
１０３　ノートＰＣ
１３０　インターネット
１４０　他のネットワーク
２００　制御部
２０１　周辺機器制御部
２０２　ＬＡＮプロトコル制御部

２０３　制御バス

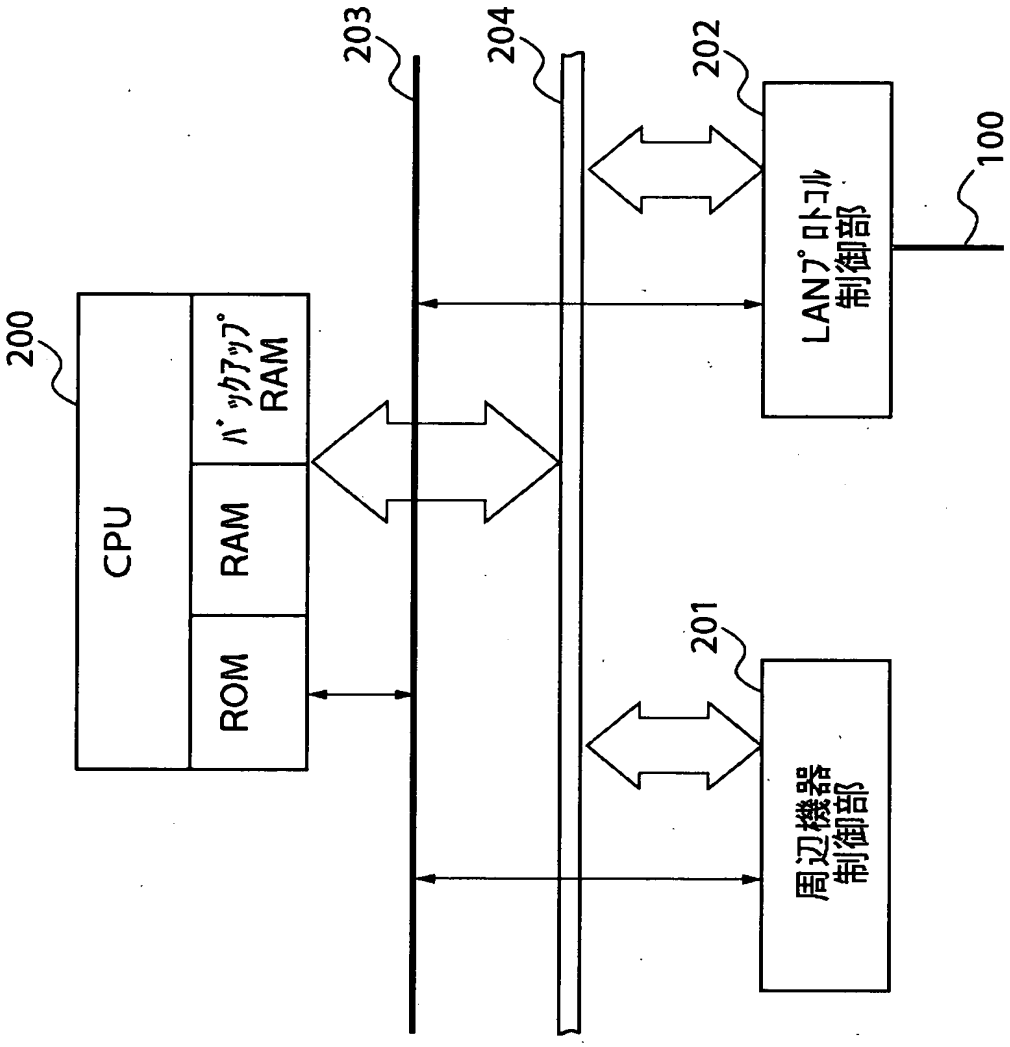
２０４　データバス

【書類名】　　図面

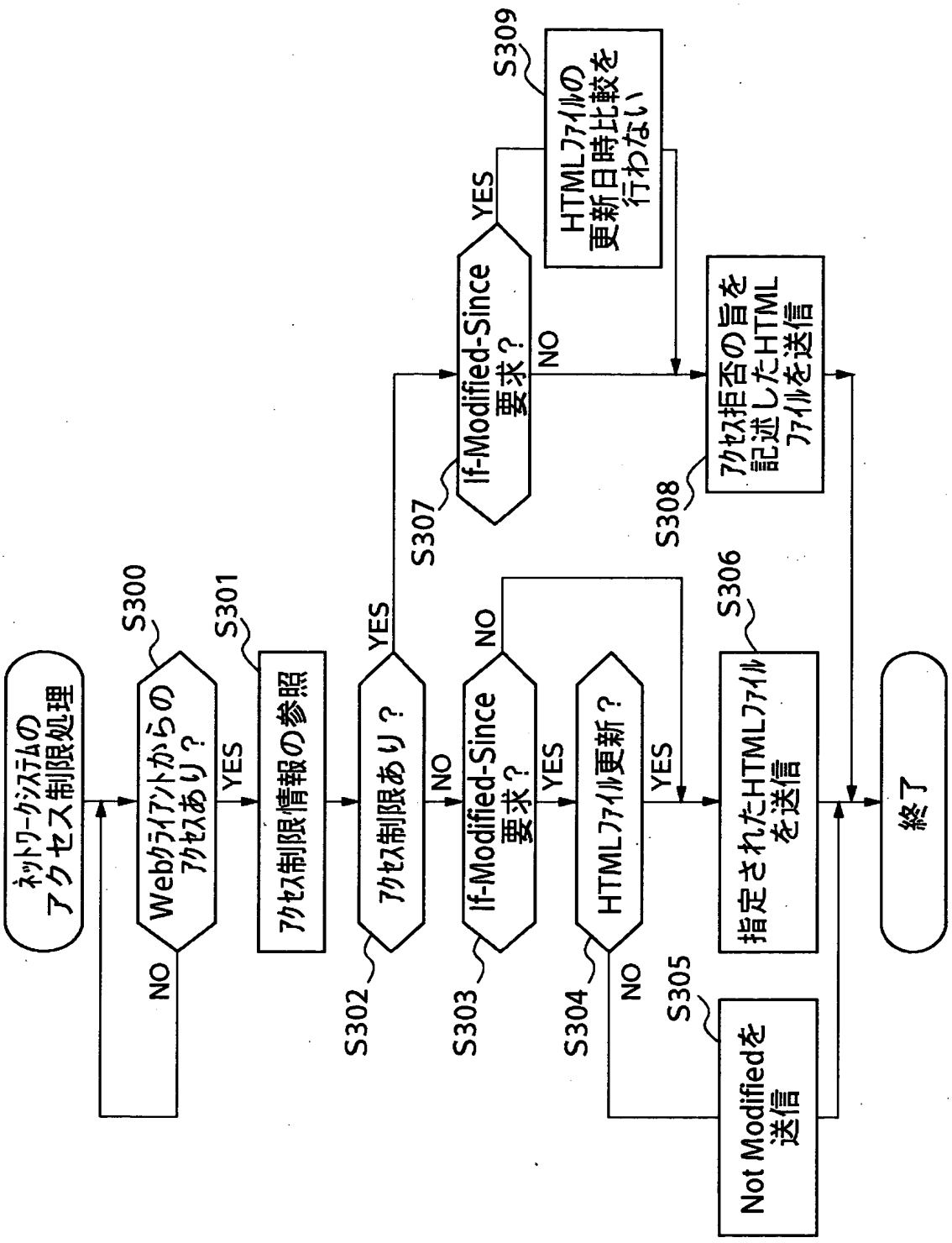
【図１】


100
100
２階
１階
104
103
113
102
112
106
DB
111
101
105
120
FireWall
130
インターネット
140

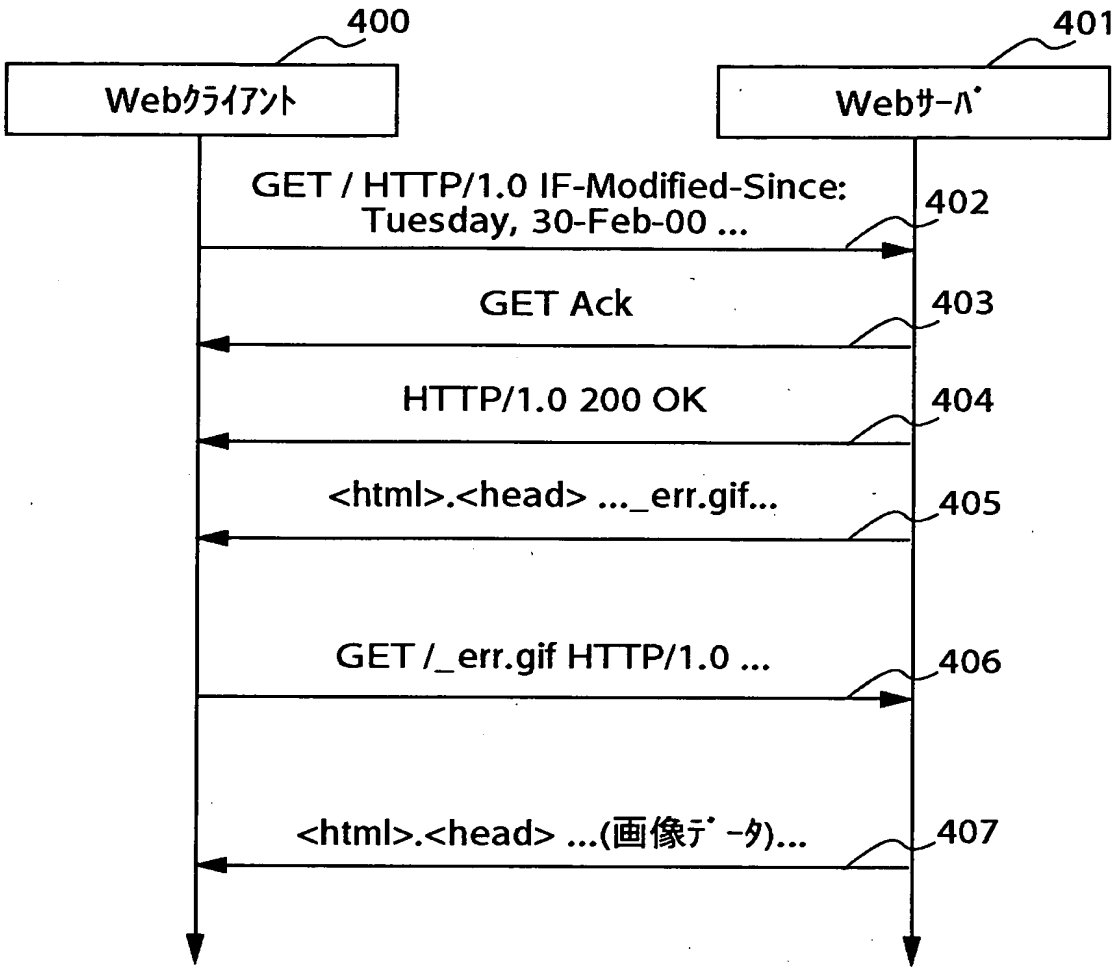
【図２】


203
204
202
100
200
CPU
RAM
ROM
バックアップ RAM
LANプロトコル 制御部
201
周辺機器 制御部

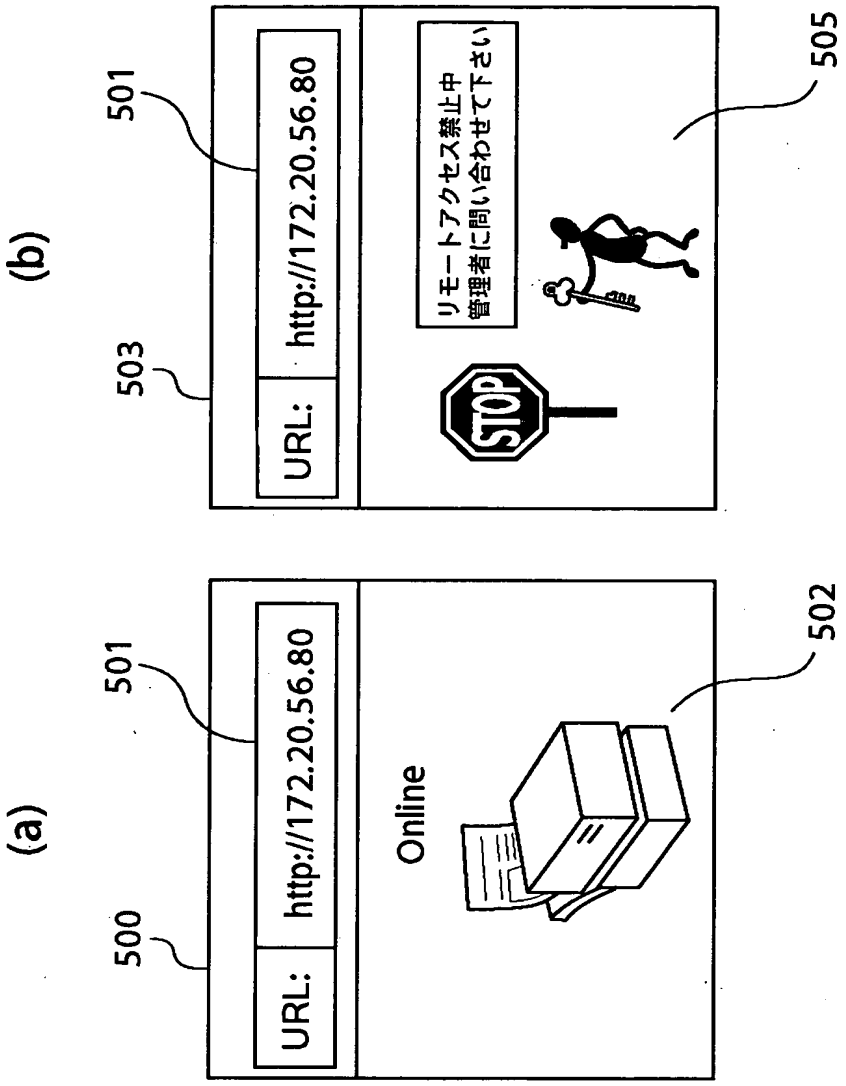
【図３】


ネットワークシステムのアクセス制限処理
S300
Webクライアントからのアクセスあり？
NO
YES
S301
アクセス制限情報の参照
S302
アクセス制限あり？
YES
NO
S303
If-Modified-Since要求？
NO
YES
S304
HTMLファイル更新？
NO
YES
S305
Not Modifiedを送信
S306
指定されたHTMLファイルを送信
S307
If-Modified-Since要求？
YES
NO
S308
アクセス拒否の旨を記述したHTMLファイルを送信
S309
HTMLファイルの更新日時比較を行わない
終了

【図４】


400
401
Webｸﾗｲｱﾝﾄ
Webｻｰﾊﾞ
GET / HTTP/1.0 IF-Modified-Since:
Tuesday, 30-Feb-00 ...
402
GET Ack
403
HTTP/1.0 200 OK
404
<html>.<head> ..._err.gif...
405
GET /_err.gif HTTP/1.0 ...
406
<html>.<head> ...(画像ﾃﾞｰﾀ)...
407

【図５】


(a)
500
501
URL:
http://172.20.56.80
Online
502
(b)
501
503
URL:
http://172.20.56.80
リモートアクセス禁止中
管理者に問い合わせて下さい
STOP
505

【書類名】　　要約書

【要約】

【課題】　ネットワークデバイスへの最新のアクセス制限の理由を明確、且つ確実にユーザに通知することができ、更にユーザに通知する表示用データの量を低減することができるネットワークシステム、Ｗｅｂサーバへのアクセス制限方法、記憶媒体、ネットワークデバイス及びその制御方法、並びにプログラムを提供する。

【解決手段】　ＬＡＮ１００には、複数のネットワークデバイスと、複数のコンピュータとが接続されている。ネットワークデバイスの少なくとも１つには、Ｗｅｂサーバ機能が搭載されており、コンピュータの少なくとも１つには、Ｗｅｂクライアントが搭載されている。Ｗｅｂサーバへのアクセスを制限することが決定しているときには、Ｗｅｂサーバへのアクセスが制限されていることを示すＨＴＭＬファイル（図５（ｂ））をＷｅｂクライアントに通知する。Ｗｅｂクライアントは通知されたＨＴＭＬファイルによって、Ｗｅｂサーバへのアクセス制限及びその理由等をユーザに確実に通知することができる。

【選択図】　　図３

認定・付加情報

特許出願の番号	特願２００１－１４１７７４
受付番号	５０１００６８４４１０
書類名	特許願
担当官	第三担当上席　　００９２
作成日	平成１３年　５月２５日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子３丁目３０番２号
【氏名又は名称】	キヤノン株式会社

【代理人】　申請人

【識別番号】	100081880
【住所又は居所】	東京都港区虎ノ門１丁目１７番１号　虎ノ門５森ビル　渡部国際特許事務所
【氏名又は名称】	渡部　敏彦

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社